Rapport semestriel du 30 août 1986

Schaff, Sylvie

Publication date:
1986

Document Version
le PDF de l'éditeur

FAST 1

Rapport semestriel du 30 août 1986

Sylvie Schaff
Attachée de Recherches
au C.R.I.D.

Le texte qui suit présente des résultats des Actions Nationales de Recherches en soutien à FAST (Services du Premier Ministre - Programmation de la Politique Scientifique). La responsabilité scientifique est assumée par un auteur.

Chapitre V - La preuve des opérations télématiques

Section 1 - L'authentification

Paragraphe 1 - L'authentification dans les opérations télématiques
A. les fonctions de la signature
B. les conditions de validité de la signature

Paragraphe 2 - La recevabilité des nouvelles techniques d'authentification

Paragraphe 3 - La force probante des nouvelles techniques d'authentification

Section 2 - La preuve du contenu de 1'opération

Paragraphe 1 - La nécessité d'un écrit
A. La règle de 1'original
B. Les exceptions au principe
C. La preuve par tous moyens

Paragraphe 2 - La recevabilité des documents télématiques
A. L'unilatéralité de la preuve
B. La recevabilité de la preuve télématique
C. La force probante des dcuments télématiques

CHAPITRE V - LA PREUVE DES OPERATIONS TELEMATIQUES

Les services télématiques professionnels, comme toutes les opérations télématiques, vont se heurter au problème de la preuve.

L'utilisation de cette technique soulève en fait deux questions :
- avec qui suis-je en contact ? En effet, les parties communiquent ici sans se voir ni s'entendre, sans qu'une signature les renseigne sur l'identité de leur partenaire ;

- quel est le contenu exact de l'opération réalisée ? La télématique, qui a pour avantage d'établir un contact en temps réel, de fournir rapidement une réponse, de transmettre des données à grande vitesse, de supprimer le support papier, a justement comme inconvénient de supprimer les traces matérielles de l'opération et donc d'établir à posteriori ses termes exacts.

Ces deux problèmes, celui de l'authentification et de la preuve du contenu des opérations télématiques seront détaillés dans les deux sections du présent chapitre.

Section 1 : L'authentification

L'authentification a trois fonctions : l'identification de l'auteur d'un message, l'indication de sa volonté de s'approprier le contenu de ce message, et la preuve de ces deux éléments.

Traditionnellement, l'authentification est effectuée au moyen d'une signature manuscrite apposée au bas du document à authentifier. Celle-ci remplit une fonction importante sur le plan juridique, ce qui explique qu'elle est soumise à des conditions strictes.

Dans le domaine de la télématique, on a pu penser que le code personnel de l'utilisateur ou les autres techniques d'authentification constituaient une sorte de signature, et pourraient avoir des effets similaires. L'analyse révèle cependant qu'il n'en est pas ainsi.

Paragraphe 1 : L'authentification dans les opérations télématiques

L'authentification ou identification en matière télématique se distingue des situations habituelles en ce qu'elle s'effectue de façon automatique et en temps réel(1). Dès qu'il introduit

son code, l'utilisateur est reconnu par le système, qui lui donne alors accès au réseau. Une signature par contre sera le plus souvent vérifiée par une personne, un employé de la banque par exemple), bien après que le document n'ait été signé (lors d'une contestation, lors d'un paiement, ...).

L'identification automatique s'effectue par une comparaison entre les données qui sont introduites dans le système et celles qu'il possède déjà en mémoire. Lorsque ces données sont identiques (introduction d'un code) ou qu'elles présentent un écart suffisamment petit (reconnaissance de caractéristiques physiques), l'ordinateur considère la personne comme identifiée et lui permet l'accès.

La reconnaissance de la personne au moyen d'un code est la méthode la plus largement utilisée aujourd'hui. Les avantages de cette méthode sont sa simplicité technologique, le faible volume des données de référence (généralement quatre chiffres par personne) et sa fiabilité (un fraudeur a seulement 3 chances sur 10000 de pénétrer dans le système). Elle présente par contre trois inconvénients graves : elle n'apporte aucune preuve de l'opération effectuée ; si un fraudeur vole le code, il est sûr de pénétrer dans le système ; enfin, quand ce code est utilisé en conjonction avec une carte magnétique (télématique bancaire essentiellement), il existe un risque que l'algorithme de cryptage soit découvert.

Une seconde méthode d'identification assez couramment utilisée est la cryptographie, c'est-à-dire le codage d'un texte de façon à le rendre incompréhensible à tout autre que son destinataire, qui procède à son décodage grâce à une "clé" confidentielle. Cette méthode a de plus l'avantage de protéger la confidentialité du message s'il est intercepté par des tiers au cours de la transmission.

Il existe des systèmes de cryptographie dits "symétriques", où émetteur et destinataire ont la même clé, et les systèmes "asymétriques". Pour ces derniers, chaque utilisateur reçoit deux clés, une clé publique que chacun peut connaitre en consultant l'annuaire ad hoc et une clé secrète, connue de lui seul. Chaque message est alors encrypté deux fois (une fois par la clé publique du destinataire et une seconde fois par la clé secrète de l'émetteur) et décrypté en deux temps (d'abord par la clé secrète du destinataire, puis par la clé publique de l'émetteur).

La cryptographie présente une grande sécurité, et c'est pourquoi elle est utilisée pour les transmissions nécessitant un degré de confidentialité élevé. Ainsi les transferts électroniques de fonds sont-ils généralement effectués sur des systèmes à cryptographie asymétrique. C'est en particulier la méthode utilisée sur le système SWIFT(2).

La cryptographie a cependant l'inconvénient de nécessiter une installation coûteuse, et de constituer une procédure d'authentification lente.

Pour pallier à ces défauts, on a élaboré des systèmes de reconnaissance des caractéristiques physiques des personnes, mais qui demeurent pour l'instant au stade expérimental(3).

La reconnaissance vocale par exemple se heurte à plusieurs difficultés. Ainsi, la voix d'un individu est fluctuante (selon son humeur, sa santé, ...) et les performances du système s'en trouvent diminuées. De plus, cette technique ne fonctionne pas dans une ambiance bruyante (rue, hall...) mais par contre répond à un enregistrement au magnétophone.

Le système le plus prometteur actuellement est celui de la reconnaissance dynamique de la signature. En effet, plusieurs systèmes ont été étudiés et certains d'entre eux sont déjà opérationnels, ou sur le point de l'être. Leur principe est de capter le mouvement du crayon pendant la signature, puis de calculer et de mémoriser dans l'ordinateur les caractéristiques de la signature (par exemple, le nombre de fois où la vitesse verticale change de sens).

En plus du fait que les performances de ce système sont bonnes (taux de fiabilité de 99%), il présente deux avantages considérables :
- la signature étant un acte habituel, il devrait être facilement accepté par le public ;

- le papier sur lequel est apposé la signature peut être conservé, à des fins de preuve notamment.

Il faut noter ici que pour que le système soit efficace, une personne doit toujours signer de la même manière, et donc renoncer à sa liberté de changer de signature quand bon lui semble. On remarque d'ailleurs que les performances du système sont meilleures pour les personnes ayant déjà acquis le réflexe de signer, c'est-à-dire en général, agées de plus de 35 ou 40 ans.

Enfin d'autres expériences dans ce domaine sont menées actuellement, mais sans que l'on escompte un résultat avant de nombreuses années. On peut citer ici la reconnaissance de l'iris, de la morphologie du visage, de la forme de la main, de la composition du sang, de l'odeur du corps, du bruit de la démarche,...

Les méthodes d'identification électronique sont susceptibles d'utilisations très diversifiées, comme par exemple l'accès à des lieux protégés, à un réseau de données ou le paiement. On estime d'ailleurs que ces méthodes vont se diffuser largement dans les cinq prochaines années, et en particulier la reconnaissance des

empreintes digitales (pour les applications de haute sécurité) et la reconnaissance dynamique de la signature (pour les applications grand public). Mais avant de devenir vraiment usuelles, ces méthodes d'identification doivent vaincre plusieurs obstacles tels que l'insuffisance des performances des systèmes, leur coût trop élevé, et l'absence d'accord entre les différents partenaires (banques, commerçants, industriels, ...) sur leur utilisation et les normes applicables.

Paragraphe 2 : La recevabilité des nouvelles techniques d'authentification

A. Les fonctions de la signature

Par son origine historique, la signature est tout d'abord un moyen d'établir la présence physique du signataire à la rédaction d'un acte(4).Cette fonction se traduit, dans les conditions de validité d'une signature, par l'exigence qu'une signature soit manuscrite (ce qui exclut tous les procédés mécaniques ou électroniques de signature).

Pour les opérations télématiques, cette fonction n'est plus adaptée puisque l'on cherche au contraire à identifier avec certitude un interlocuteur éloigné. C'est là une première distinction entre la signature au sens traditionnel du terme et le code de l'utilisateur d'un service télématique.

La seconde fonction de la signature est d'indiquer l'identité du signataire, ce qui explique qu'elle soit soumise à certaines règles de forme (indiciation du nom du signataire, en toutes lettres, ...). C'est ce que nous appelerons sa fonction d'identification. Le code utilisé dans les opérations télématiques, dans la mesure où il est personnel et confidentiel, remplit parfaitement cette seconde fonction.

La signature indique enfin la volonté du signataire : par cet acte, il montre son accord avec le contenu du document. Cette fonction est évidemment liée à la précédente, puisque si une personne se charge d'une obligation, il importe de déterminer son identité avec certitude.

Un code ne remplit pas non plus cette seconde fonction, puisqu'il est introduit avant toute opération pour avoir accès au service. Il est donc nécessaire de prévoir une procédure supplémentaire, accomplie à la fin de l'opération, si l'on veut s'assurer de l'accord de celui qui l'a effectuée.

C'est la solution adoptée par certains fournisseurs par exemple pour des achats payés à un terminal point de vente des transactions conclues par voie télématique ou les guichets automatiques Mister Cash en Belgique, où l'utilisateur doit, à la

fin de l'opération, appuyer sur la touche "OK" pour finaliser son accord. Ici, seul l'acte d'appuyer sur la touche "OK" peut être assimilé à une signature dans ce sens qu'il indique la volonté de l'utilisateur de s'approprier le conteun du message, et en cela l"authentifie" au sens propre du terme.

B. Les conditions de validité de la signature

1) "Pour être valable, la signature suppose l'apposition du nom; elle doit reproduire le nom du signataire"(5). Il ressort de cette affirmation qu'un code ne serait pas une signature valable dans l'état actuel de notre droit.

En effet, la règle traditionnelle veut que la signature soit nécessairement ".... la traduction écrite d'un vocable désignant oralement le signataire...." et interdit l'utilisation d'autres procédés tels que les sceaux ou l'apposition des seules initiales.

Ainsi la Cour de Cassation indiquait, dans l'arrêt du 7 janvier 1955 : "la signature au sens de l'article 970 du Code Civil est la marque manuscrite par laquelle le testateur révèle habituellement sa personnalité aux tiers" (6).

La sévérité de cette position a cependant été critiquée, surtout avec la multiplication des documents écrits et par là des occasions de signer. On a ainsi pu affirmer que la signature d'un testament olographe ne constituait pas une solennité, mais une condition destinée à garantir la sincérité de ce testament et qu'en conséquence, toute formule équivalente garantissant cette sincérité devait être acceptée (7).

Reprenant le même argument, ne pourrait-on pas dire aujourd'hui que le code, lorsqu'il remplit les mêmes fonctions qu'une signature, devrait être considéré comme son équivalent ? Cette position est renforcée par la reconnaissance dans de nombreux pays de la validité des modes de signature mécaniques ou électroniques dans le domaine commercial (8) et par le fait qu'il n'existe aucune définition légale de la signature.

En fait, ce qui est important ici est de savoir si le signe utilisé (signature, tampon, griffe, code ....) a la même portée qu'une signature au sens traditionnel du terme, c'est-à-dire qu'il indique, avec au moins les mêmes garanties d'authenticité, l'identité de celui qui l'utilise et sa volonté de s'approprier le contenu du document qui le porte.

Pour le déterminer, le juge s'aidera des circonstances de fait, et en particulier des habitudes dans le domaine considéré (domaine commercial, télématique, ...). C'est ainsi que la Cour de Cassation française, dans un arrêt de principe rendu le 24 juin 1952, a décidé que peu importe le caractère de la signature

"...dès lors qu'elle permet d'établir avec certitude l'identité de l'auteur de ce document et sa volonté d'en approuver les dispositions" (9).

On peut donc en déduire qu'une signature qui n'indique pas exactement le nom du signataire serait tout de même valable. Cependant en droit belge, une signature doit nécessairement être constituée de caractères d'écriture (10), de sorte que la qualification de signature ne s'applique pas à un code.

2) En second lieu, selon les termes de l'article 970 du Code Civil, une signature doit être manuscrite afin de témoigner de la présence physique du signataire. Il est admis que cette disposition, prévue en matière de testament olographe, vaut pour tout acte.
Elle exclut donc qu'une signature soit apposée par une autre personne que le signataire. On doit remarquer ici que cette condition est respectée dans la plupart des services télématiques, qui attribuent à leurs clients des codes personnels et confidentiels et considèrent le titulaire comme entièrement responsable de son utilisation. Les services bancaires en sont un exemple d'application particulièrement strict.

Pour les autres services télématiques, la consultation de banques de données par exemple, il arrive que plusieurs personnes soient titulaires du même code. Le fournisseur du service insiste alors toujours pour connaitre l'identité de ces titulaires, qui assument chacun une responsabilité personnelle sur l'utilisation du code.

Les utilisateurs de services télématiques sont d'ailleurs engagés par contrat à veiller à la confidentialité de leur code. Ces dispositions montrent que comme une signature, un code est considéré comme étant personnel et par là identifiant son titulaire.

C'est cette nécessité d'une signature manuscrite qui a fait pendant longtemps dénier toute valeur aux signatures au moyen de tampons, de griffes ...(11). En effet, celles-ci ne témoignent pas de la présence physique du signataire. On peut argumenter ici qu'en matière de télématique, hors cas de négligence ou de fraude, l'utilisation du code révèle la présence physique du signataire devant le terminal, présumément pendant toute la durée de la communication, et que le code se rapproche donc sur ce point d'une signature.

Toujours est-il qu'aujourd'hui, l'expansion des affaires a multiplié les cas où une signature est requise et la nécessité d'une signature manuscrite n'est guère compatible avec l'accroissement du rythme des transactions.
C'est pourquoi la pratique s'est développée, surtout en France, de signer les effets de commerce au moyen de griffe ou de fac-similé. Malgré la condamnation de cette pratique par la Cour

de Cassation, les banques continuèrent à accepter les effets non signés de la main du signataire, et le législateur intervint en édictant le 16 juin 1966 la "loi relative à l'emploi de procédés non manuscrits pour apposer certaines signatures sur les effets de commerce et chèques"(12).

Sur le plan international, il faut signaler ici les travaux menés au sein de la CNUDCI sur la facilitation des procédures du commerce international, et en particulier la Recommandation adoptée lors de la dix-huitième session (3-21 juin 1985) qui enjoint aux gouvernements "de réexaminer l'exigence légale d'une signature manuscrite ou de toute autre méthode d'authentification sur papier pour les documents commerciaux afin de permettre, le cas échéant, l'utilisation de moyens électroniques d'authnetification"(13).

En droit belge, le principe demeure qu'une signature doit être manuscrite et une autre sorte de signature entrainerait la nullité de l'acte sur lequel elle est apposée (14). Il n'existe que de très rares exceptions à cette règle, strictement définies par la loi et concernant la signature d'un grand nombre de documents identiques (signature des administrateurs sur les actions et obligations d'une société, signature du gouverneur de la Banque Nationale et du trésorier sur les billets de banque). Il en résulte qu'en droit belge actuel, un code ne saurait en aucun cas valoir une signature.

3) Enfin selon les principes traditionnels, une signature ne fait foi que pour le document sur lequel elle a été matériellement apposée, et la jurisprudence a ainsi constamment refusé de reconnaitre la validité d'une signature obtenue à l'aide d'un papier carbone (sans lui nier une certaine valeur probante, dans certains cas) (15). Cette position est motivée par le risque que le double sur lequel figure cette signature ne reflète pas la volonté du signataire, par exemple si ce double ne comprend pas les mêmes termes que l'original sur lequel est la signature a été matériellement apposée.

Or en matière de télématique, il n'existe pas de document papier qui constitue un original au sens habituel du terme, et l'introduction du code dans le système ne laisse pas une trace comparable à une signature.

Peut-on considérer la chaine de signaux binaires qui représente toute opération télématique comme un tel "document" ? Cela demanderait une extension particulièrement aventureuse de la notion de document, et il est à craindre que notre système légal ne soit pas encore prêt à l'accepter (cf. infra l'acceptation de documents informatiques comme moyens de preuve).

Doit-on alors estimer que le document est constitué par la première copie sur imprimante de cette chaine de signaux ? Cette solution doit également être rejetée. Tout d'abord parce que de

nombreuses opérations télématiques ne donnent pas lieu à de telles copies, en particulier les opérations interactives comme la consultation de banques de données, et que l'absence de cette copie ne doit pas permettre de mettre en doute la réalité de l'opération concernée. Ensuite cette copie est localisée chez l'une des parties, et l'autre partie étant absente lors de son exécution, n'a pas l'occasion d'y apposer matériellement sa signature ou son numéro de code. Une telle exigence reviendrait à ôter tout intérêt à la télématique, qui est justement d'éviter la circulation du papier et de pouvoir "traiter" à distance.

Plus que la signature, il apparait que c'est ici le paiement qui manifeste l'accord de l'utilisateur avec le contenu de l'opération télématique réalisée : lorsqu'il approuve les montants facturés, il les règle alors qu'en cas de désaccord il refusera de payer avant d'avoir pu s'expliquer avec le fournisseur du service.
C'est d'ailleurs la solution retenue dans les contrats, les fournisseurs de service s'engageant à conserver les informations relatives aux opérations effectuées pendant un certain délai, au-delà duquel les contestations par les clients ne seront pplus acceptées(16).

Aussi, il apparait que le code et la signature ont pour seul point commun d'identifier une personne. Un code ne peut donc pas, sur le plan juridique, être assimilé à une signature et sa valeur juridique, en tant que tel, est nulle (17).

Mais cela ne signifie pas que le code n'a aucune valeur. En particulier, il est une technique d'identification relativement sûre (lorsqu'il n'y a pas eu de négligence ou de fraude), et un élément de preuve (le fournisseur qui démontre l'utilisation du code peut attribuer une opération déterminée au client qui en est titulaire).
C'est pourquoi, parlant de code, il nous apparait plus juste de le qualifier de moyen d'identification (d'une personne) plutôt que d'une méthode d'authentification (d'un document). Cette conclusion est d'ailleurs renforcée par le fait que le code est introduit avant toute opération, qu'il ne peut donc authentifier "a priori". Cela ne signifie pas que l'authentification télématique soit impossible (la seule condition à respecter est d'être effectuée <u>après</u> la transaction), mais il faut bien constater que ce que l'on appelle aujourd'hui des moyens d'authentification sont le plus souvent utilisés à des fins d'identification seulement, bien que leur utilisation à des fins d'authentification soit possible.

<u>Paragraphe 3 : La force probante des nouvelles techniques d'identification</u>

A.Les exigences légales

Sur le plan de la preuve, le droit établit une distinction entre un fait juridique et un acte juridique : alors qu'un fait juridique peut être prouvé par tout moyen (présomption, aveu, témoignage,...), un acte juridique ne peut être prouvé que par un écrit signé (art. 1341 C. civ.). Comment les distingue-t-on ? Le critère généralement admis est que les conséquences juridiques d'un acte juridique ont été voulues par son auteur, alors qu'il n'a pas prévu les conséquences juridiques d'un fait (18). On considère en particulier, et bien que cette solution ait donné lieu à de violentes critiques, que l'exécution d'un acte juridique constitue en elle-même un fait juridique (19).

En application de ces principes, une opération télématique peut être qualifiée d'acte juridique lorsqu'il s'agit d'une transaction conclue par voie télématique, et de fait juridique dans tous les autres cas.

En particulier, les opérations effectuées dans le cadre des services professionnels que nous avons analysés ainsi que les transferts électroniques de fonds peuvent être qualifiés de faits juridiques puisqu'ils sont accomplis en exécution de contrats préalables conclus sous une forme écrite traditionnelle.

Certains auteurs se sont cependant demandés si ces opérations devaient être considérées comme des actes d'exécution, qui peuvent être prouvés par tous moyens, ou comme des conventions particulieres conclues dans le cadre d'une convention générale, et dont la preuve ne pourrait être faite que par écrit.

Dans la pratique, il faut remarquer que cette seconde solution présente des difficultés du fait de l'absence d'écrit dans les opérations télématiques, et aboutit surtout à compliquer une matière qui l'est déjà suffisamment (cf. infra section 2).

Il n'est cependant pas exclu que dans l'avenir, les contrats-cadre soient conclus par voie télématique, et soient alors soumis au régime probatoire des actes juridiques, en particulier à la nécessité d'un écrit signé avec le problème de la signature mentionné plus haut. Du fait cependant qu'en matière commerciale tous les modes de preuve sont admis, lorsque les transmissions télématiques pourront être qualifiées de commerciales, ce qui est souvent le cas en matière de télématique professionnelle, l'absence de signature au sens traditionnel du terme pourra être palliée par l'utilisation de codes ou de clés de cryptographie, sauf dans les cas où une signature est requise par les usages ou par la réglementation.

B. La position de la jurisprudence

Il n'existe pas encore de jurisprudene relative à la force probante des nouvelles techniques d'authentification, mais on peut essayer de l'envisager à partir de la position qu'avaient pris les tribunaux lors de l'introduction de méthodes d'authentification moins récentes, essentiellement celles utilisées lors de transactions passées par télex ou par téléphone (17).

Il ressort de l'analyse de la jurisprudence de plusieurs pays que si les tribunaux accordent une grande fiabilité aux transactions conclues par telex, il n'en est pas de même pour celles qui sont conclues par téléphone (21). Cette position s'explique par le fait que le telex laisse une trace écrite qui identifie l'appelant, le destinataire, la date et l'heure de la transmission alors que ce n'est pas le cas pour les communications téléphoniques.

Il est évidemment à craindre que la même objection soit faite aux services télématiques. Introduire l'obligation d'imprimer toute communication supprimerait tout intérêt à cette nouvelle technique, et la solution la plus réaliste consiste à reconnaitre la valeur probante des documents informatiques. C'est d'ailleurs dans cette voie que se dirigent actuellement la plupart des pays, sous l'influence des travaux menés au sein du Conseil de l'Europe et de la CNUDCI.

C. Conventions d'authentification

Pour éliminer, ou du moins amenuiser les incertitudes quant à la force probante des méthodes d'authentification qu'elles utilisent, les parties peuvent, en vertu de l'article 1134 du Code civil, insérer dans leur contrat une clause qui reconnait une force probante particulière à cette méthode (22).

Ainsi les parties qui ont des relations télématiques suivies peuvent juger utile de faire figurer une telle clause dans leur convention par exemple dans la convention de base conclue entre une banque et une entreprise avec laquelle existe une liaison télématique, ou dans le règlement d'un réseau de transfert électronique de fonds auquel les banques participantes doivent adhérer. On remarque cependant que ces clauses sont rares etlimitées à certains types d'opérations (présentant une certaine valeur financière) et que les contrats d'abonnement aux banques de données par exemple ne contiennent jamais de telles clauses.

L'article 3 al. 5 de la convention "Liaison interactive Tele-Link" de la Banque Bruxelles Lambert prévoit ainsi :
"Il est expressément convenu que le résultat des calculs combinés composant la signature électronique, tels qu'ils sont détaillés dans la brochure technique, sera considéré par les deux parties comme preuve valable et irréfutable de l'identité et de l'accord

des donneurs d'ordre, pour toutes les instructions données sous cette signature électronique". Un article semblable est repris da,s 1'article 5 al. 2 de la convetion G-Line de la Société Générale de Banque.

Les clauses d'authentification prévoient, ou devraient prévoir, la durée pendant laquelle les parties conserveront les documents qui portent la trace des techniques d'authentification utilisées. Quant à 1'effet de ces clauses on peut dire, par analogie avec la jurisprudence en matière de telex (23), que le fait d'avoir suivi les procédures d'authentification usuelles ne devrait pas dispenser le récepteur de message de faire des vérifications supplémentaires lorsque le contenu du message ou ses circonstances sont douteux ou inhabituels pour autant qu'il puisse s'en rendre compte.

De manière générale, on constate que ces clauses permettent aux parties à la fois une grande liberté dans les moyens d'authentification utilisables et une sécurité juridique suffisante. En effet, dès qu'une technique d'authentification sera relativement répandue dans la pratique, il est probable qu'elle soit objectivement fiable et qu'en conséquence un tribunal lui reconnaitrait une force probante privilégiée. Un tel cas ne s'est cependant, à notre connaissance, pas encore présenté devant les tribunaux.

Section 2 : La preuve du contenu de l'opération

Alors que dans la première section, on s'est soucié d'identifier l'auteur de l'opération télématique, cette section sera consacrée à cette opération elle-même et aux moyens ouverts aux parties pour prouver son contenu exact en cas de litige.

Bien que certains problèmes leur soient communs, chaque type de service télématique est susceptible de connaître des litiges qui lui sont plus spécifiques. Ainsi les services de documentation et les services de fourniture d'énergie informatique verront naitre des litiges au sujet du service utilisé (les banques de données ou les programmes proposés ont des tarifs différents, et l'utilisateur comme le fournisseur ont intérêt à connaître quelle banque de données ou quel programme a été effectivement consulté) ou au sujet de la durée de la consultation (qui a également un effet sur la redevance).

Les services de télétraitement connaissent des contestations sur la durée effective d'un traitement, le type de système requis pour l'effectuer, le délai de livraison.

Enfin les services de communication quant à eux devront répondre de la perte de messages, ou de la durée anormale de leur transmission.

Ces exemples démontrent l'importance pour les parties, fournisseur et utilisateur du service, de pouvoir apporter la preuve de leurs dires. Comment peuvent-ils le faire ?

Nous avons vu que notre droit distingue sur ce point les actes et les faits juridiques, et que si la convention-cadre constitue sans aucun doute un acte juridique, qui ne peut être prouvé que par un écrit, il existe encore des doutes pour les opérations télématiques effectuées en application de cette convention (cf. supra). La question de la preuve des opérations télématiques doit en fait être abordée sous deux angles. Le premier consiste à se placer du côté de la législation existante, et à se demander comment elle va s'appliquer à ces opérations. Le second consiste au contraire à partir de la pratique existante, et à rechercher les dispositions légales applicables. C'est pourquoi nous analyserons en premier lieu la nécessité d'un écrit comme mode de preuve(paragraphe 1), puis la recevabilité des documents télématiques (paragraphe 2).

Paragraphe 1 : La nécessité d'un écrit

A. La règle de l'original

La preuve est réglementée en droit belge par les articles 1315 à 1369 du Code civil, qui consacrent cinq modes de preuve : l'écrit, l'aveu, le serment décisoire, le témoignage et les présomptions (24).

Parmi ces modes de preuve, l'écrit est celui qui a la plus grande valeur : en présence d'un écrit, le juge ne peut recourir à sa propre conviction, et un écrit ne peut être renversé que par un autre écrit (art. 1341 C.civ.).

La valeur de l'écrit est encore renforcée par les dispositions de l'article 1341 du Code Civil, selon lequel : "Il doit être passé acte devant notaire ou sous signature privée de toute chose excédant la somme ou la valeur de 3000 francs...". Il en résulte que la preuve de la plupart des opérations télématiques, dont le montant est bien supérieur à 3000 francs, ne pourra se faire que par écrit. Il est donc important de définir ici ce que l'on entend par un écrit.

Pour être valide, un écrit doit être complet, original et signé manuscritement. Nous avons déjà abordé la question de la signature en matière télématique (cf. supra), mais il demeure un problème plus fondamental : existe-t-il alors un écrit ?

Par exemple, la bande-journal sur laquelle une banque enregistre toutes les opérations constitue-t-elle un écrit au sens juridique du terme ? De même pour les enregistrements que

conservent les serveurs de banques de données, les fournisseurs de services de messagerie électronique ou d'énergie informatique?

Au-delà de ces cas particuliers, c'est toute la question de la recevabilité des documents informatiques qui est posée et l'on constate que bien que dans de nombreux pays seul un écrit original a une valeur probatoire devant un tribunal, cette règle a subi les adaptations requises par les pratiques actuelles.

En effet, l'utilisation de microfilms et d'enregistrements informatiques présente de nombreux avantages pour la conservation des documents (gain d'espace, plus grande durabilité du support,...) et il existe plusieurs pays qui acceptent la présentation d'un tel enregistrement comme preuve à la place de l'original(25).

Dans ce sens, la Recommandation R(81) 20 du Conseil de l'Europe adoptée le 11 décembre 1981 par le Comité des Ministres demande aux gouvernements des Etats-membres d'adapter leur législation afin d'accepter la conservation de certains documents, notamment commerciaux, sous forme de micrographie ou d'enregistrements informatiques et de reconnaitre à ces reproductions une valeur égale à celle d'un original lorsqu'elles satisfont à un certain nombre de règles générales énoncées en annexe de la Recommandation (Point III de la Recommandation).

Exposées succintement, ces règles générales prévoient qu'un tel enregistrement doit :
"a. correspondre fidèlement soit aux documents originaux, soit à l'information qui est à l'origine de l'enregistrement ;
b. être effectué de façon systématique et sans lacune ;
c. être effectué selon des instructions de travail établies conformément à la législation nationale et conservées aussi longtemps que les reproductions ou enregistrements ;
d. être conservé avec soin, dans un ordre systématique et protégé contre toute altération"(art. 3 al. 1 de l'Annexe).

Lorsque l'original est détruit après après sa reproduction, ce qui est très courant afin de profiter réellement des avantages que présente l'informatique, il est en outre nécessaire de conserver les informations suivantes :
"a. l'identité des personnes responsables de la reproduction ou de l'enregistrement et de celles les ayant effectuées ;
b. nature du document ;
c. lieu et date de la reproduction ou de l'enregistrement ;
d. les défauts éventuels constatés pendant la reproduction ou l'enregistrement." (Art. 3 al. 2 de l'Annexe).

Les enregistrements répondant à ces conditions sont alors admis comme preuve devant les tribunaux et présumés être fidèles et complets, sauf preuve du contraire (Art. 2 de l'Annexe).

La Recommandation demande en outre aux Etats-membres d'examiner la possibilité de supprimer l'exigence d'une preuve par écrit, ou du moins de la limiter aux opérations portant sur un montant élevé (728 DTS au moment de sa mise en oeuvre, selon le point I de la Recommandation).

Les lois nationales et cette Recommandation partent cependant du principe qu'il existe ou a existé un original, qui a été éventuellement détruit après son enregistrement. Or dans le domaine télématique, l'opération est entièrement effectuée par informatique et il n'existe pas de document-papier constituant un original au sens habituel du terme. On s'est alors demandé si la sortie sur imprimante ou la visualisation sur écran devait être considérée comme un original ou comme une copie de l'enregistrement stocké sur un support informatique (26).

Si dans de nombreux pays cette question n'a même pas été posée, ceux qui l'ont abordée l'ont fait de façon pragmatique : seul un document lisible par un être humain peut être présenté devant un tribunal, ce qui exclut tout enregistrement informatique.

Ainsi aux Etats-Unis, les règles de la preuve ont été modifiées et assimilent maintenant une sortie sur imprimante à un document original. En France, la loi du 12 juillet 1980 relative à la preuve des actes juridiques, reconnait la valeur probante d'une copie "lorsque la partie ou le dépositaire n'a pas conservé l'original et présente une copie qui en est la reproduction non seulement fidèle mais également durable. Est réputée durable toute reproduction indélébile de l'original qui entraine une modification irréversible du support". Cette loi admet ainsi la valeur probante d'un microfilm ou d'une photocopie (27). Un enregistrement informatique pourrait sans doute leur être assimilé sur ce point, dans la mesure où il constitue un document fidèle et durable au sens de la loi.

Dans les opérations télématiques, l'argument peut être présenté qu'il n'existe pas d'original qui a été détruit, mais que l'enregistrement informatique est cet original lui-même. Cet argument nous apparait comme d'autant plus favorable à la reconnaissance de la valeur probante de l'enregistrement informatique.

B. Les exceptions au principe

Il existe plusieurs exceptions au principe de la nécessité d'un écrit, qui permettent de contourner dans un certain nombre de cas la difficulté que présente l'absence d'écrit en matière télématique.

1)En premier lieu, par interprétation a contrario de l'article 1341 du Code civil, les transactions dont la valeur

est inférieure à 3000F peuvent être prouvées par tous moyens. La question ici est de savoir si le montant qu'il faut prendre en considération est celui qui est indiqué dans la convention-cadre (c'est-à-dire le prix de l'abonnement au service) ou celui de chaque opération prise individuellement.

Dans le premier cas, du fait que la convention-cadre fait pour l'instant toujours l'objet d'un écrit, il ne se pose aucun problème de preuve quelque soit le montant de l'abonnement. Cette situation pourrait cependant changer, avec la diffusion et la banalisation de services de ce type, et le régime de la preuve serait alors celui qui est applicable aux aux transactions conclues par voie télématique(28).

La seconde hypothèse consiste à considérer que le montant de 3000F doit s'apprécier pour chaque opération prise isolément. La première conséquence en est que le nombre de cas où un écrit est nécessaire sera très inférieur au nombre d'opérations effectuées, notamment pour les services de messagerie électronique et de documnetation, ce qui aboutit à appliquer le régime de la preuve par tous moyens à la majorité des opérations télématiques.

On peut s'interroger ensuite sur la nature juridique de ces opérations. Soit il s'agit d'actes juridiques, de conventions distinctes conclues dans le cadre formé par la convention originale, dont la preuve doit en conséquence nécessairement être apportée par écrit. Le principe est alors celui qui est applicable en matière de transactions conclues par voie télématique.
La plupart des auteurs considèrent cependant qu'il s'agit de faits juridiques accomplis en exécution de la convention originale et qui peuvent donc être prouvés par tous moyens quelque soit leur montant (29).

Cette dernière solution nous apparait comme la plus souhaitable. En effet, l'utilisation de services télématiques peut difficilement être qualifiée "d'acte juridique" puisqu'elle n'est pas destinée dans la plupart des cas à provoquer des conséquences juridiques, et si celles-ci surviennent, elles n'auront le plus souvent pas été prévues par l'utilisateur. Il faut signaler cependant que certains services télématiques offrent la possibilité de conclure des actes juridiques, comme par exemple l'achat de biens de consommation par les services télématiques grand-public. Dans ces cas, la nécessité d'un écrit ne nous semble pas contestable, mais c'est à travaers la remise en cause de la notion d'écrit, et en particulier l'acceptation de la force probante des documents informatiques (cf. supra p. 8) qu'elle nous semble devoir être résolue.

Enfin, sur un plan plus pragmatique, cette solution permet de résoudre la difficulté posée par l'absence d'un écrit dans les opérations télématiques : il existe un contrat écrit, acte juridique qui fait preuve de la convention des parties et en

exécution duquel les parties réalisent des opérations télématiques, faits juridiques que l'on peut prouver par tous moyens, et en particulier par des documents informatisés. On peut d'ailleurs considérer que les paiements effectués à ces occasions entrent dans le cadre du contrat principal, qui contient des dispositions à leur égard (périodicité, prix prévus en annexe, ...).

Dans l'hypothèse où dans l'avenir, les conventions-cadre devaient également être conclues par télématique, il est évidemment nécessaire de mettre en place dès à présent des mécanismes juridiques assurant la sécurité des parties. Des travaux dans ce sens ont été entrepris au sein des organismes internationaux pour reconnaitre la validité des documents informatiques comme mode de preuve, et l'élaboration d'usages professionnels dans ce domaine permet de définir les droits et obligations des parties aux opérations télématiques (30).

2) Une deuxième exception au principe de la preuve écrite existe pour les opérations passées entre commerçantsqui peuvent, selon les régles du droit commercial, être prouvées par tous moyens sauf dans certains cas spécifiques prévus par la loi (31). Cette exception s'applique à un bon nombre d'opérations télématiques professionnelles, qui pourront en conséquence être prouvées par témoignages, documents informatiques, ... et tout autre moyen que le juge acceptera de recevoir.

En cas d'acte mixte, c'est-à-dire conclu entre un commerçant et un non commerçant, le régime de preuve applicable est déterminé par la qualité du défendeur. L'utilisateur pourra ainsi dans la plupart des cas utiliser les règles de preuve du droit commercial contre le fournisseur du service (il peut cependant exister une exception pour les services publics, en particulier les banques de données proposées par l'administration).

Le fournisseur du service, par contre, devra dans certains cas avoir recours contre son client aux modes de preuve du droit civil, et devra alors produire un écrit pour toute transaction dont la valeur est supérieure à 3000F. Nous retrouvons ici la situation analysée dans le point précédent.

3) Les règles de preuve de l'article 1341 n'étant pas d'ordre public, il est également possible pour les parties de prévoir dans leur convention les modes de preuve qui seront applicables. Ce genre de clause est extrèmement fréquent dans le secteur bancaire et prévoit par exemple :

> "la bande-journal ou le support d'information équivalent sur lesquels sont enregistrées les données relatives à toutes les opérations à chaque guichet automatique ou chaque terminal point de vente constitue un procédé de preuve par écrit contraignant et suffisant"(32).

Ces conventions de preuve se rapprochent des conventions d'authentification analysées auparavant. Comme elles, elles sont l'expression de la force du consensualisme dans notre droit et sont valides tant qu'elles ne contreviennent pas à une disposition d'ordre public ou ne marquent pas un déséquilibre des parties (clauses léonines). Dans un tel cas, ces clauses peuvent être déclarées nulles par le juge, qui appliquera soit les dispositions obligatoires dans ce domaine, soit le droit commun.

4) Le Code Civil prévoit expressément qu'il peut être fait exception à ses dispositions lorsqu'il a été impossible pour le créancier "... de se procurer une preuve littérale de l'obligation qui a été contractée envers lui" (art. 1348 C. civ).

Selon plusieurs auteurs, l'utilisation d'un système télématique constituerait un cas d'impossibilité de se procurer une preuve littérale qui justifierait la non-application de l'article 1341 (33). Cette interprétation se fonde en particulier sur la modification en France de l'article 1348 par la loi du 12 juillet 1980 relative à la preuve des actes juridiques. Dans sa nouvelle version, l'article 1348 prévoit qu'il est fait exception à l'article 1341 lorsque ".... l'une des parties n'a pas la possibilité matérielle ou morale de se procurer une preuve littérale de l'acte juridique".

Or, selon Mme Chamoux en particulier, l'utilisation d'un système télématique constituerait sans aucun doute un cas dans lequel il y a impossibilité matérielle de se procurer un écrit. Cette analyse est d'ailleurs confirmée par la tendance jurisprudentielle actuelle en France, favorable à un régime probatoire extensif pour les opérations télématiques.

Cette position est cependant critiquable. En effet, la télématique ne constitue qu'un mode particulier de télécommunication, les parties auraient pu en choisir un autre, tel le courrier ou le telex qui laissent une trace écrite, et c'est pourquoi d'autres auteurs refusent de reconnaitre dans ce cas une impossibilité matérielle de produire un écrit et d'appliquer l'exception de l'article 1348 aux opérations télématiques (34).

De plus, parmi les quatre cas d'application de l'exception prévus par l'article 1348, on peut difficilement en trouver un qui se rapproche, même de loin, de notre hypothèse. En effet, cette exception s'applique, selon les termes mêmes du Code civil, dans des situations imprévisibles (tels que les délits ou quasi-délits ou les accidents survenant à la suite d'événements de force majeure) ou lorsque le créancier a perdu le titre qui lui servait de preuve littérale à la suite de tels accidents.

Appliquer cette exception aux opérations télématiques impliquerait donc une interprétation tout à fait nouvelle de l'article 1348 et de la notion d'impossibilité de se procurer une preuve littérale : en effet, l'impossibilité due à un événement

imprévu ne peut pas être assimilée à l'impossibilité due à des conditions matérielles parfaitement connues à l'avance et pour lesquelles il existe des possibilités de substitution.

Il nous parait en conséquence douteux qu'une partie qui se prévaudrait aujourd'hui de l'exception de l'article 1348 pour justifier l'absence d'écrit dans une opération télématique serait entendue par le tribunal. Néanmoins, elle trouverait certainement parmi les autres principes juridiques applicables (distinction acte et fait juridique, preuve des actes commerciaux, ...) une possibilité de présenter les éléments de preuve dont elle dispose. De plus, si la notion d'impossibilité n'est pas applicable aujourd'hui aux opérations télématiques, on peut envisager soit que son interprétation change, notamment sous l'influence de Mme Chamoux et de M. Syx, de manière à considérer la technique télématique comme l'un des cas d'impossibilité visés, soit que le recours à cette notion devienne inutile du fait de l'acceptation des documents télématiques comme des écrits originaux. C'est dans cette seconde direction que les travaux des organismes internationaux s'orientent actuellement et il est donc probable que c'est cette solution qui sera finalement adoptée.

5) Enfin les règles de l'article 1341 reçoivent exception lorsqu'il existe un commencement de preuve par écrit (art. 1347 C. civ). Celui-ci est défini par le Code civil comme "... tout acte écrit qui est émané de celui contre lequel la demande est formée ... et qui rend vraisemblable le fait allégué".

Sur le plan de la pratique, les juges requièrent que le commencement de preuve par écrit soit complété par une autre preuve, écrite ou non. Nous retrouvons donc ici le problème de la définition d'un écrit, analysé plus haut. Il apparait que pour la jurisprudence française très souple dans ce domaine, une bande magnétique peut être considérée comme un commencement de preuve d'une opération télématique(35). Par contre en droit belge, les conditions d'acceptation d'un commencement de preuve par écrit demeurent celles édictées par le Code Civil, et il est douteux qu'une partie pourrait se prévaloir d'un enregistrement télématique comme commencement de preuve par écrit.

Pour M. Syx cependant(36), ces enregistrements devraient être acceptés comme tels. En effet, bien qu'ils ne constituent pas des "écrits" au sens traditionnel du terme, les enregistrements informatiques présentent une valeur probante certaine dans ce sens que l'information significative est enregistrée par le système au moment même où elle est exprimée et par un logiciel fixe que ne peuvent manipuler ni le client, ni le fournisseur du service, ni le serveur informatique, dans un environnement technique qui depuis 1979 a prouvé sa grande fiabilité. M. Syx en conclut que les enregistrements

informatiques constituent des "procédés de preuve écrit innomés" c'est-à-dire non prévus par la loi mais réunissant toutes les conditions nécessaires pour être considérés comme des commencements de preuve par écrit(37).

C. La preuve par tous moyens

Lorsque les opérations télématiques peuvent être prouvées par tous moyens, par exemple parce qu'elles sont qualifiées de faits juridiques ou qu'elles ont lieu entre commerçants, quels sont alors les moyens de preuve à la disposition des parties ?

La preuve par aveu, par serment et par témoignage , telle qu'elle est prévue au Code civil, ne présente pas en matière télématique de spécificité particulière, et ne sera pas étudiée ici (38). On peut par contre s'interroger plus longuement sur les présomptions qui pourront être retenues dans ce domaine.

Selon 1'article 1349 du Code civil, les présomptions sont "... des conséquences que ... le magistrat tire d'un fait connu à un fait inconnu". La forme de ces faits et la manière dont ils viennent à la connaissance du juge ne sont précisées par le Code, et la jurisprudence lui reconnait toute liberté pour rechercher les présomptions où il le veut, même dans des actes étrangers aux parties (39), et dans des documents qui ne répondent pas à la définition juridique d'un écrit. La seule condition posée est que ces présomptions soient "graves, précises et concordantes"(art. 1353 C. civ.), ce qui relève de l'appréciation souveraine des juges du fonds. Il a ainsi en particulier été décidé qu'une bande magnétique enregistrée constituait un fait connu, d'où le juge pouvait tirer une présomption valide (40).

On peut donc considérer qu'un document télématique serait suffisant pour permettre au juge d'en tirer des présomptions quant aux conditions d'exécution du service (service utilisé, durée, pannes, ...). Cette méthode repose cependant sur l'hypothèse que les documents en question sont suffisamment fiables et complets pour permettre une décision juste. Or, selon plusieurs auteurs, les procédés actuellement utilisés ne rempliraient pas cette condition (41).

Paragraphe 2 : la recevabilité des documents télématiques

Nous avons vu dans la première section de ce chapitre que les procédés d'authentification utilisés en télématique, s'ils sont aussi sûrs qu'une signature, sont cependant considérés comme étant encore insuffisants et que des recherches sont effectuées pour permettre une identification sans doute possible (en particulier par les caractéristiques physiques de 1'individu).

Ainsi le fournisseur de service qui entend faire payer un client en apportant la preuve que c'est son numéro de code qui a été utilisé n'est pas sûr qu'en fait, ce code n'a pas été utilisé par un tiers. Pour parer à cette éventualité, le contrat prévoit que l'utilisateur a une responsabilité personnelle sur ce code, et devra payer toute opération effectuée sous ce numéro.

Si l'opération est le fait d'un tiers qui a profité de la négligence de l'utilisateur, il est compréhensible que ce dernier en supporte les conséquences. Mais l'utilisateur peut être tout à fait innocent, le tiers peut s'être introduit sur le réseau de manière frauduleuse et il est alors grave que l'utilisateur ne dispose d'aucun moyen de prouver sa bonne foi.

L'authentification n'est qu'un des aspects du problème de la preuve. En effet, même s'il est d'accord sur le fait de l'interrogation, comment l'utilisateur peut-il prouver que la facture qu'on lui adresse ne correspond pas aux opérations effectuées (service utilisé et durée d'utilisation essentiellement) ? Comment peut-il prouver qu'il a effectivement envoyé un message qui n'est pas arrivé, ce qui peut avoir de graves conséquences notamment dans le domaine commercial et ralentir considérablement l'utilisation de la télématique ?

Un moyen de preuve possible est la bande magnétique sur laquelle est enregistrée l'opération effectuée. Cette bande présente cependant, sur un plan juridique, deux inconvénients graves : elle est en possession du serveur télématique uniquement, et il n'a aucune obligation de la conserver ou de la déposer où que ce soit.

A. L'unilatéralité de la preuve

Notre droit en effet condamne la preuve unilatérale dans les relations synallagmatiques. Les auteurs du Code civil ont voulu que les deux parties à une convention se trouvent sur un pied d'égalité, et en particulier que chacune d'elles ait la même possibilité de faire valoir ses droits (42). Cette volonté apparait dans l'article 1325 du Code, qui stipule qu'une convention n'est valable qu'autant qu'elle a été faite en autant d'originaux qu'il y a de parties distinctes.

Lorsque cette condition n'est pas remplie, la jurisprudence se prononce pour la nullité du titre, justifiée par le fait que les parties n'ont pas eu les mêmes facilités probatoires a priori et considère le titre annulé éventuellement comme commencement de preuve par écrit (43).

Cette jurisprudence, tout à fait fondée du fait que la partie en possession de la preuve unilatérale peut l'avoir falsifiée, revêt une importance particulière dans le domaine télématique où la bande magnétique est souvent la seule preuve disponible.

Pour pallier à cette difficulté, on a songé à confier la tâche probatoire à un tiers. Sur le réseau télématique, un des tiers envisageables est le transmetteur, qui de plus, du fait du monopole des télécommunications en vigueur aujourd'hui dans la plupart des pays européens, présente une garantie d'extranéité et de neutralité par rapport aux parties.

Cependant, cette solution a été appliquée, puis abandonnée en Allemagne pour le réseau Bildschirmtext au motif qu'elle présente le grave inconvénient de concentrer tous les renseignements relatifs aux opérations télématiques entre les mains d'une seule entité, qui de plus fait partie de l'Etat, ce qui a soulevé des inquiétudes en matière de protection de la vie privée notamment.

Une second exemple de l'intervention d'un tiers dans l'opération télématique est fourni par le réseau "Bancontact". Bancontact est une société juridiquement indépendante qui met à la disposition des banques et de leurs clients un réseau de guichets automatiques et de terminaux point de vente. Le client, qui effectue l'opération, n'entre cependant jamais en contact avec cette société. Du fait cependant que Bancontact est une société coopérative créée et administrée par les banques participantes, il est difficile de l'assimiler à un tiers présentant les garanties de neutralité souhaitées.

Une solution acceptable semble donc être de laisser aux serveurs, indépendamment ou non, le soin de conserver les bandes magnétiques contenant le relevé des opérations télématiques et de leur imposer une obligation de les conserver en sûreté pendant un certain délai. Cette obligation est d'ailleurs déjà acceptée par certains serveurs qui indiquent dans leur contrats que les bandes seront conservées pendant une durée déterminée (souvent deux mois) au-delà de laquelle les clients renoncent à toute contestation. Il apparait cependant que les conditions d'enregistrement et de conservation de ces bandes devraient, pour plus de sûreté, être fixées par la loi ou par un accord international. A cet égard, les règles énoncées dans la Recommandation R(81) 20 du Conseil de l'Europe précitée pourraient être étendues aux services télématiques.

B. La recevabilité de la preuve télématique

Au niveau international, on remarque que la recevabilité des documents télématiques comme moyen de preuve dans les différents pays dépend du régime de la preuve dans ce pays. De façon schématique, on relève trois types de règles juridiques en matière d'établissement de la preuve, fondées sur des traditions et des pratiques juridiques différentes : la libre présentation de tout moyen de preuve, une liste exhaustive des moyens de preuve recevables, et la règle du témoignage indirect ("Hearsay rule")(44).

Un certain nombre de pays tout d'abord acceptent la libre présentation de tous les éléments de preuve pertinents. Si une contestation s'élève quant à l'exactitude de l'un des éléments présentés, le tribunal décide alors de la valeur probante à lui accorder. Dans ces pays, la présentation d'enregistrements informatiques comme moyens de preuve ne soulève aucune difficulté.

De nombreux pays de tradition civiliste, et la Belgique en particulier, ont établi une liste exhaustive des moyens de preuve recevables. Cette liste comprend toujours l'écrit, mais jamais l'enregistrement informatique bien que des réformes soient envisagées ou commencent à être mises en oeuvre. Nous avons vu (cf. supra) que l'assimilation d'un tel enregistrement à un écrit est difficile, et une intervention législative est donc nécessaire pour qu'il constitue un moyen de preuve recevable.

Cette restriction est cependant le plus souvent limitée au civil. Dans les matières pénales ou commerciales par exemple, tous les moyens de preuve sont admis et un enregistrement informatique est alors accepté. C'est en particulier le cas en Belgique.

Enfin les pays de common law suivent en matière de preuve la règle du témoignage indirect, ou "hearsay rule". Dans ces pays, la procédure judiciaire est orale et contradictoire et un témoin ne peut attester que de faits auxquels il a personnellement assisté afin que la partie adverse puisse procéder à un contre-interrogatoire.

Il existe cependant de nombreuses exceptions à cette règle, notamment dans le domaine commercial où un enregistrement effectué dans le cadre normal des activités peut être accepté comme preuve s'il n'existe aucun témoin qui pourrait en certifier l'exactitude en se fondant sur sa connaissance personnelle.

En ce qui concerne les enregistrements informatiques, ils sont acceptés comme preuve dans les pays de common law dans deux cas :
- soit parce que l'on considère que l'exception en faveur des enregistrements commerciaux leur est applicable ;

- soit parce que ce pays a adopté une loi stipulant expressément que les enregistrements informatiques sont des moyens de preuve valides, que le litige soit commercial ou non (par contre, il peut exister une distinction pour les affaires pénales).

Après avoir examiné la recevabilité d'un enregistrement informatique comme mode de preuve sur un plan juridique , il convient de se poser la question d'un point de vue plus pratique : un tel enregistrement constitue-t-il une preuve suffisamment fiable ?

C. La force probante des documents télématiques

Cette question peut être considérée sous deux aspects, en premier lieu d'un point de vue général (un enregistrement informatique est-il un moyen de preuve acceptable) et en second lieu d'un point de vue particulier (tel enregistrement donné est-il suffisant et fiable dans telle affaire).

On retrouve ici la distinction entre trois systèmes d'attitude relevés précedemment (45).

les pays qui acceptent tous les éléments pertinents reconnaissent que les enregistrements informatiques sont suffisamment fiables pour être admis comme preuve par un tribunal. En présence d'un tel enregistrement, le tribunal décidera de la valeur probante à lui accorder.

Par contre les pays dans lesquels existe une liste exhaustive des moyens de preuve recevables n'ont pas encore reconnu la fiabilité des enregistrements informatiques comme modes de preuve, mais des réformes sur ce point sont imminentes. Dans une affaire déterminée, un juge pourra néanmoins prendre en compte un tel enregistrement, par exemple parce qu'il fait naitre une présomption (cf. supra).

Enfin dans les systèmes de common law, selon le mécanisme qui leur est propre, il a été dégagé des critères qui permettent à un juge de déterminer si un enregistrement informatique a une force probante suffisante. On relève trois catégories de tels critères, les premiers ayant trait au matériel informatique utilisé, les seconds aux procédures d'enregistrement et les derniers au traitement informatique lui-même (programmation, stockage, sortie d'imprimante).

Ainsi la partie qui présente un enregistrement informatique à titre de preuve doit démontrer :
- que le matériel utilisé "... était tel que l'on peut considérer qu'il a fonctionné de manière satisfaisante" (matériel adapté au traitement, compatibilité des divers éléments, logiciel approprié, ...)(46);
- que lors de l'introduction des données dans l'ordinateur les procédures destinées à garantir l'exactitude de l'enregistrement ont été respectées, par exemple qu'il s'agit d'un enregistrement ayant eu lieu dans le cadre des activités normales de l'entreprise ou dans un délai raisonnable après que le fait se soit produit ;
- enfin que les méthodes de traitement, de stockage et de sortie d'imprimante garantissent la fiabilité de l'enregistrement, notamment en ce qui concerne la programmation, l'utilisation et le contrôle de l'ordinateur.

Dans la pratique, il peut être assez difficile de décrire aujourd'hui à un tribunal certains modes de traitement

informatique extrèmement sophistiqués, et c'est pourquoi les tribunaux acceptent de plus en plus souvent une déclaration générale que le système a fonctionné normalement.
De plus, contrairement aux règles de la procédure orale, les lois admettent que cette déclaration peut être faite par écrit, sous serment, par une personne connaissant bien le système informatique concerné et que son témoignage oral peut être limité aux cas ou l'exactitude des données est contestée (48).

Aussi est-il rare aujourd'hui qu'un tribunal de common law refuse d'examiner un enregistrement informatique, même si son exactitude est contestée. Un tel refus est alors fondé sur la non-observation des critères indiqués, en particulier l'utilisation d'un matériel qui ne correspond pas à l'état actuel des techniques, une gestion non professionnelle de ce matériel ou des procédures inacceptables, c'est-à-dire en fait l'absence de force probante de l'enregistrement en question.

Même s'il est admis qu'un enregistrement informatique est en principe suffisamment fiable pour constituer un moyen de preuve recevable, le juge conserve toujours le pouvoir d'apprécier la valeur d'un enregistrement qui lui est présenté.

En effet, les données indiquées sur cet enregistrement peuvent être inexactes, même si le système informatique dans son ensemble a fonctionné correctement, et le juge doit pouvoir en décider lorsque leur exactitude est contestée (48).

Nous avons vu que la Recommandation R(81) 20 du Conseil de l'Europe établit une présomption d'exactitude pour les enregistrements informatiques "... des livres, documents et données pouvant en vertu de la loi être conservés sur ordinateur et qui ont été effectués conformément aux procédures énoncées..." dans ladite Recommandation (49). Il nous semble que cette règle pourrait être étendue aux opérations télématiques. La partie qui conteste l'exactitude de l'enregistrement devra alors renverser la présomption en prouvant soit l'inexactitude des données, soit le défaut du système informatique utilisé.

Quant aux critères d'évaluation de la fiabilité d'un enregistrement informatique, il apparait que les critères retenus par les tribunaux de common law, et qui sont repris dans la Recommandation du Conseil de l'Europe sont les principaux critères qui doivent être pris en considération. On peut cependant tenir compte également des mesures de sécurité prises au niveau de l'ordinateur et du réseau de transmission.

En conclusion, il apparait qu'aujourd'hui, dans la plupart des pays, un tribunal est libre d'évaluer la force probante des enregistrements informatiques qui lui sont présentés sur la base des éléments de preuve dont il dispose.

NOTES

1) T. Schwab et M. d'Alençon, "L'authentification des personnes", texte de l'exposé présenté lors du séminaire International sur "Les terminaux Point de vente, Fraude et Sécurité", organisé par l'OROS à Paris les 18 et 19 octobre 1984.

2) B. Amory et X. Thunis, "Authentification de l'origine et du contenu des transactions sans papier et questions de responsabilité en droit continental", exposé présenté lors de la Conférence sur "les Transactions commerciales internationales assistées par ordinateur et droit dans la CEE", organisée par CELIM à Bruxelles les 17 et 18 mars 1986 p. 43.

3) Schwab et d'Alençon, précité n° 1

4) M. Van Quickenborne, "Quelques réflexions sur la signature des actes sous seing privé", note sous Cass. 2! juin 1982, RCJB 1985 p. 69.

5) Id. p. 71.

6) Ann. not. 1955, 307. Dans ce sens, voir les autres références indiquées par M. Van Quickenborne, précité n° 4, p. 73 n° 27.

7) De Page et Dekkers, VIII, 2 n° 860, D, 2°, p. 1009, cité par M. Van Quickenborne, précité n° 4, p. 76 n° 36.

8) Voir ainsi en France la loi du 16 juin 1966 "relative à l'emploi de procédés non-manuscrits pour apposer certaines signatures sur les effets de commerce et le chèque", et les travaux de la CNUDCI dans ce domaine.

9) Sem. Jurid., 1952, 7179 note P. Voisin, D. 1952? 5B ; RTDC, 1952, 531 note R. Savatier.

10) Van Quickenborne, précité n° 4, p. 83.

11) Id., p. 85

12) Id., p. 87

13) Assemblée Générale, Documents Officiels : Quarantième session supplément n° 17 (A/40/17), Nations Unies, New York, 1985.

14) Van Quickenborne, précité n°4, p. 88.

15) Id., p. 89.

16) M.G. Choisy, "Banque de Données ; Aspects contractuels", Agence de l'Informatique, 1982, p. 589.

17) M. Vasseur, "Aspects juridiques des nouveaux moyens de paiement", Revue de la Banque, 1982, p. 589.

18) Y. Poullet et X. Thunis, "Introduction aux aspects juridiques de la télématique", in "La Télématique : aspects techniques, juridiques et socio-politiques", Story Scientia, Gand (1984) Tome 1, p. 159.

19) B. Amory et X. Thunis, "Introduction aux aspects juridiques de la télématique", in "La Télématique : aspects techniques, juridiques et socio-politiques", Story-Scientia, Gand (1984), Tome 1, p. 159.

20) Id. p. 47

21) Id. p. 48

22) Id. p. 49 ; voir aussi X. Linand de Bellefonds et A. Hollande, "Droit de l'Informatique", Masson, Paris (1984), p. 125.

23) D. Carton, "Aspects juridiques des ordres de paiement transmis par telex", DISEP, Octobre 1985, p. 4.

24) M. Goyens et J. Laffineur, "Questions juridiques liées à l'introduction de la télématique grand-public", Rapport du Centre de Droit de la consommation de l'U.C.L., octobre 1985, p. 148.

25) CNUDCI, "Valeur juridique des enregistrements informatiques", 21 février 1985, A/CN.9/265 p. 14.

26) Id., p. 15.

27) Van Quickenborne, précité n° 18, tome 2 p. 261.

28) M. Goyens et J. Laffineur, précité n° 24, p. 151.

29) Y. Poullet et X. Thunis, "Reflexions sur le mouvement électronique de fonds", in :"La Télématique : aspects techniques, juridiques et socio-politiques", précité n° 18, tome 2, p. 261.
M. Goyens et J. Laffineur, précité n° 24, p. 152
contra : voir D. Syx, "Het bewijsrecht en de informatica : een verkenning van een recente problematieke", basistext i.v.m. de cursus "De computer en zijn toepassings problemen in het recht", les van 26 fevruary 1985, Faculteit Rechtsgeleedheid RUG, p. 18.

30) Cf. travaux menés au sein de la CNUDCI, du Conseil de l'Europe, des Communautés Européennes ainsi que les études par le Groupement Français des Fournisseurs d'Information en ligne et l'European Association of Information Services.

31) Livre 1, Titre IV du Code de Commerce.

32) M. Goyens et J. Laffineur, précité n° 24, p. 154 ; Convention Bancontact, art. 6 al. 3.
Y. Poullet et X. Thunis, précité n° 18, p. 161 ; art. 5 de la Convention G. Line de la Société Générale de Banque ; art. 12 du contrat Terminal de Paiement de la société Bancontact.

33) M. Goyens et J. Laffineur, précité n° 24, p. 155.

34) M. Goyens et J. Laffineur, précité n° 24, p. 155.

35) Id. p. 156.

36) D. Syx, précité n° 29, p. 21.

37) D. Syx, "Le transfert électronique de fonds : le droit hésitant face à une réalité galopante" in : "La télématique", précité n° 18, tome 2, p. 233-239.

38) M. Goyens et J. Laffineur, précité n° 24, p. 156.

39) Cass., 28 avril 1842, Pas. 1842, p. 362.

40) Cass. 24 novembre 1961, Pas. 1962, p. 367 ; Cass., 29 octobre 1962, Pas. 1963, p. 272.

41) M. Goyens et J. Laffineur, précité n° 24, p. 157.

42) Van Quickenborne, précité n° 4, p. 94.

43) Id. p. 98-99.

44) CNUDCI, précité n° 26, p. 9.

45) Id., p. 11.

46) Id.

47) Id. p. 12.

48) Id. p. 13.

49) Art. 2 de l'Annexe de la Recommandation.

30)